EmpMonitor On Azure

Deployment Guide

EmpMonitor
Keep your workforce united

Table of Contents

EmpMonitor on Azure Overview

EmpMonitor provides the best employee monitoring solutions and also offers flexible deployment options. All EmpMonitor solutions are available to be deployed as a private cloud option on Microsoft's enterprise-ready Azure platform. This deployment guide will help you understand what you can expect from Azure deployment of EmpMonitor and also gives you the step-by-step guidance with preconditions for installations, technical and support details.

Benefits of Deploying EmpMonitor on Azure

If you prefer cloud deployments but have concerns about the safety and compliance or you want an on-premise deployment but sit back due to the cost and hassle of the infrastructure then Azure deployment is the right option for you. Making the transition to host EmpMonitor on Azure will give you a lot of infrastructure benefits.

Competitive Pricing
Only pay for the resources you consume, no extra or upfront cost. Also, if you are already using Windows Server and SQL server then you can save even more. EmpMonitor offers a very reasonable price of $0.052/hr* for the configuration of a standard deployment (B2S instance: 2 CPU cores, 4GB RAM, 8GB SSD - supporting up to 100 users).

Maximum Coverage
Azure has the most coverage globally than any other cloud services provider. It covers approx 54 regions and 140 countries. Global customers have the advantage to save on infrastructure costs and other complexity by hosting in an Azure data center. You can also pair Availability Zones and regions for the EmpMonitor setup.
Note: Currently, all regions are not available on EmpMonitor.

Easy Deployment
Launch the EmpMonitor Deployment from EmpMonitor Azure Marketplace page to create an EmpMonitor Machine or if you prefer the deployment through API calls, PowerShell console, ARM templates to automatically deploy using the Azure portal.

Premium Storage and Optimisation
Most of the EmpMonitor Azure Deployments come with SSD's specially designed for low latency dusk support and high-performance. In addition to that, EmpMonitor also enables you to choose from a range of options for special purposes like Compute/Storage Optimized instances.

Agility and Scaling
EmpMonitor comes with horizontal and vertical scaling with optional auto-scaling that enables you to run down the instances up or down automatically on telemetry data with Azure Monitor.

Reliability and Disaster Recovery

Your data will remain immune to Azure's High Availability (HA), multi-geo replications redundancy, offsite disaster recovery features, and on-demand backup.

Security and Compliance

EmpMonitor has the largest portfolio in the industry when it comes to privacy, security, and transparency. Combining that with EmpMonitor's GDPR, PCI DSS, etc. enforcement makes EmpMonitor and Azure a perfect solution for government, banking, healthcare, and other regulated industries customers.

Central Management Console

No need to worry about managing the infrastructure as Azure comes with built-in support for application monitoring, patching, log analytics, backup, and site recovery. You can manage and configure all your deployments from a central location.

Prerequisites

To get started, you will need:
• An Azure account
• Your EmpMonitor license key, available from EmpMonitor Self-Hosted portal at: ----
• An SSH client like Putty if you are using Windows

Step by Step Instructions

It's very easy to get started with EmpMonitor on Azure. Just create a VM on your Azure portal, add storage and database then deploy EmpMonitor in minutes with a ready-made Debian 9 Azure Image. Below are the
step by step instructions:

Step 1-1
Visit: (need to add link)
and click the Check out EmpMonitor on Azure
Marketplace button.

- Once you are on the portal, click on the GET IT NOW button. A window will pop-up with the title, Create the app in Azure.
- Click the Continue button.

Your Azure Portal will get launched and you will be redirected to create a virtual machine page. You might be asked to login if you aren't
already.

Step 1-2
- The Create a virtual machine page has several tabs.
- On the first tab, Basics, under Subscription pick an existing Resource category or build a new one.
- Give your virtual machine a name for example, 'EmpMonitor VM' under INSTANCE DETAILS.
- Select Password for Authentication type, near the bottom of the page. Provide your admin username and password to authenticate the account.
- Click on the Next: Disks button to continue to the next screen/tab.

Step 1-3
- On the Disks screen, keep the default options as it is.
- Note that EmpMonitor requires the primary volume to be on SSD or equivalently fast storage for deployments above 500 users.
- Click on the Next: Networking button to
  continue to the next screen/tab.

Step 1-4
EmpMonitor already comes with a Network Interface Card (NIC) pre-configured with the requisite NSG rules for use with the VM. So, you should keep the same settings on the Network Screen, unless you have special needs. Select Next: Administration button to move to next screen/tab.

Step 1-5
The Management screen helps you to switch the Tracking, Identity, and Auto-Shutdown settings. As for these we will keep the default settings. Click the Next button: Advanced to move to the next screen/tab.

Step 1-6

On the Advanced screen, you can install post-deployment extensions. Since none of this is required, you can select Next to move to the next screen/tab.

Step 1-7

Tags lets you categorize unified billing services. If you like, you can choose to use this option. We won't use any tags for the tutorial. Click on the Next button: Test + build. For all the settings Azure will run a validation test.

Step 1-8

Wait while Azure runs a search of all the settings for validation.

Step 1-9

If the checks are completed, Azure will show a message passed by the Validation unless it finds any errors. To start building the virtual machine, check all your settings and click the Create button at the bottom of the page. Instance creation will take a few minutes, depending on your settings.

Step 1-10

You will see the full message of your deployment when the deployment is full. Your newly created virtual machine will appear on the RESOURCE list. The machine's STATUS should display OK until you can proceed to the next step.

Step 1-11

Perform the steps as follows:
1. Click the All tools button on the central portal screen at the left-hand sidebar.
2. Locate and click on your Virtual Machine.
3. Click Right-side Overview Option. In the right hand side of the screen, it will open another window.

Step 1-12

The Overview screen will show a description of settings and current status of the VM. Locate the Virtual machine Public IP address. Copy or write down. We're going to use this IP in the upcoming steps.

Step 1-13

Start an SSH session. If you are on Windows, you can use an SSH tool such as Putty or a similar utility. Make sure you have access to administrative matters.

Type: ssh username@ip_addressthen press Enter.

Here, username is the Username you used for the administrator account when creating the VM. ip_addressis the public IP you copied in the previous step.

When asked for the password enter the VM's admin password and press Enter. The server will be ready in a few minutes.

Step 1-14

You will be prompted for a Role once the server is ready. Nonetheless, we need to take care of only a few other things before we can do that. Keep this command window open because you can use it at a later stage to finalize setup.

Storage Considerations

For EmpMonitor deployment, external storage is not vital. EmpMonitor, however, uses OCR screen recording file storage, and Microsoft Azure Blob Storage is an efficient, secure, scalable, and redundant solution for storing such data within Azure. At the same time, it's advisable to have external storage for deployments of over 100 users monitored.

If you are aware of the storage creation process, you may skip the next step.

Creating a Microsoft Azure Blob Storage

Step 3-1
Perform the steps as follows:
From the left side-bar, Select All Resources from your Azure Portal

- Tap on the Add option available above
- Select Storage, in the right panel from the option list.
- From the Right Panel, select the storage link.

It will lead you to the Create storage account.

Step 3-2
Similar to the several tabs available on the top. As like the create virtual machine page demonstrated in step 1. You can keep the default settings as in for quick deployment and easy processing.

- Basics, on the primary tab, click on the resource group which you want to choose or create a new group by selecting the create new link option.
- Add up a storage name, in the storage account name section beneath the details section. For example, storage name - "myempstorage"
- Select Next

Step 3-3
Enable the secure transfer option.
Next, click on "Tags" to move ahead.

Step 3-4
In accordance with the VM creation screen, categorize resources for consolidated billings using Tags.
Next, click on the Review + create button.

Step 3-5

Azure conducts a validation test for all settings and confirms with a message passed with Validation unless there are errors in it.

Review all of your settings and click the Create button near the bottom of the page to start storage creation. Creating storage could take some time.

Step 3-6

Once Azure is done it will show the message of Your deployment. You can see underneath the RESOURCE list for your newly generated room.

Database Considerations

However, using the Azure Database for PostgreSQL, external databases can increase the server's scalability and is recommended for deployments of over 100 concurrent users.

We'll teach you how to build an Azure Database for PostgreSQL with EmpMonitor to use with this demo.

Creating An Azure Database for PostgreSQL

Step 5-1

Perform the steps as follows:

- From the left panel bar, click on All Resources from Azure Portal.
- Select Add option from the top menu bar.
- Select databases, from the options right side.
- Select the Azure Database for PostgreSQL link, from the right panel.

This will lead to the deployment option.

Step 5-2
- Here is the deployment, select the way you want to use your service.
- Select the option below (as per your requirement).

Step 5-3
- On the Single Server page, select the Resource group you want to use under the first tab, Basics, or click the Create new connection below to create a new community.
- Add a name to the data in the server name field under the details section.
- To authenticate your account, add up the user name along with the secured password.
- It also allows you to include the location of your data center.
- Select Next, when done.

Step 5-4
- For consolidated bills, categorize resources using tags.
- Select Next, to continue.

Step 5-5
- Azure on the Review + create screen will give you an estimated monthly cost and other details for the database.
- To start building the database, review all your settings, and click the Create button at the bottom of the page. Production of the database could take a few minutes.

Step 5-6
- As soon as the process is done, a complete message of Deployment pop's up. A newly created Database will be available in the Resource List.

Step 5-7
Perform the steps as follows:

- From your Azure Portal, click All resources from the left-sidebar.
- From the list of resources, select the database you just created.
- A panel will open that shows all database properties. Click the Security Connection link in the Settings section.
- The connection security panel will be opened.

Click on the All services option available on the left-hand sidebar in your Azure Server.

From the resource, list selects the database you have just created.

Step 5-8
On security panel Connection:
- Switch the Enable access to "ON" for Azure services.
- DISABLE Near the bottom of the Enforce SSL link option.
- To save the changes press the Save button on top.

Finishing the Deployment

Now that you've created the storage and database, you're ready to continue the deployment process.

Step 6-1
- Go back to your SSH window (mentioned in step 1).
- Assign a name at the role prompt.
- Enter Yes, in the external database.
- After that, EmpMonitor will ask for the details regarding the database.

Step 6-2
Get the database connection details by performing the steps as follows:
- Click on the All resources menu on the Azure main interface's left-hand sidebar.
- Click the name of your database from the Resource list. A screen must open with all of the properties of the database.
- Under the Settings group, click Connection strings.

Step 6-3
- Copy or write down the server/host porting from the top string on the Connection strings panel.
- Also copy or write down a part of the user ID.

Step 6-4
- Return to the SSH window.
- Paste or type the hostname you just copied from the database, and click Enter.
- Paste or type the username of the database that you just copied, and press Enter.
- Type in Step 5-3 the password you used when creating the database, and press Enter.

Step 6-5
- Upon setup of the database, EmpMonitor will ask if you want to use Azure storage.
- Type Yes and then click Enter.
- Next, you'll need to provide the name of the Azure storage account and the login key.

Step 6-6
To get the name of the storage account and the access key, perform the steps as follows:

- Click on the All resources menu on the Azure main interface's left-hand sidebar.
- Click the name of your database from the Resource list. A screen must open with all of the properties of the database.
- Under the Settings group, click Connection strings.

Step 6-7
- Copy, or write down the name of the Storage account on the Access keys column.
- Under the desired section, copy or write down the Key.

Step 6-8

- Return to the SSH window.
- Paste or type the storage account name you just copied, and press Enter.
- Paste or type the key that you just copied, and press Enter.
- The storage set up by EmpMonitor and the server installation finalized.

Step 6-9

- Once done, you will get the https link. Copy that link or note it down.
- Now, you can close the SSH window.

Step 6-10

- Open a new window on a different browser and paste the https link that you have copied.
- You may get an SSL warning message as we have not used any SSL certificate. You can do it later on from the EmpMonitor dashboard. Most of the browsers will let you navigate through the warning.
- Click on the ADVANCED button on the page if you are using Google Chrome, and then click the Proceed link to move further.

Step 6-11

You will get EmpMonitor's welcome screen, select your timezone and language accordingly.

Step 6-12

- Now, enter an email and a password that will be used for your admin account and secure your EmpMonitor installation screen.
- Click on Continue to proceed.

Step 6-13

- Open a new browser and go to the portal. Login with your admin email and password.
- Click on the licenses tab and from the list of licenses, click on the key link under the actions column. A pop up message will display the license key.
- Copy the license key or note it down.

Step 6-14

Go back to your EmpMonitor dashboard, enter the license key, and click on the continue button.

Step 6-15

- Now, your server is ready for accepting incoming data from EmpMonitor's agent.
- Click on the option " install agents" to install the agent. In case you need help in the installation, then follow the instructions under the 'EmpMonitor Agent' section on the EmpMonitor user guide --(link)-- or watch the tutorial video -- (link)-- on the YouTube Channel.

Architecture
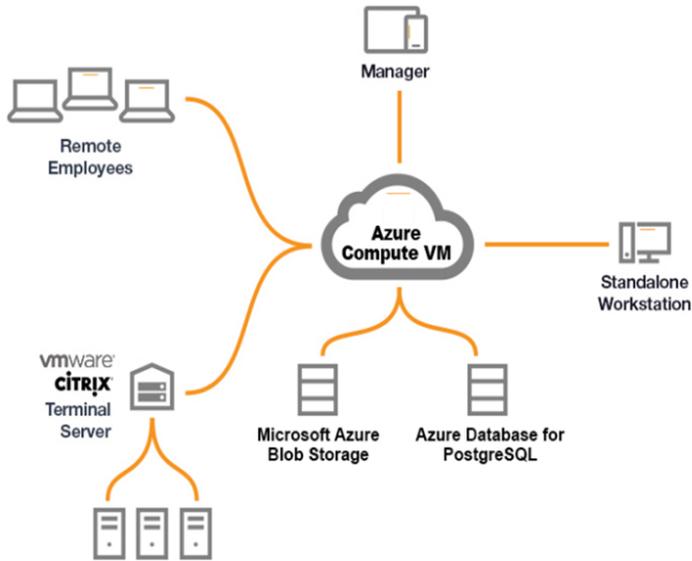
Technical Specs, Support, & Licensing

Supported Platforms	• Microsoft Windows 7, 8 and 10 (32-bit and 64-bit) • Microsoft Windows Server 2008, 2012, 2016 and 2019 • Linux Os • Mac Os
Sessions	• Stand-alone workstation / server • Terminal server (RDS)
Load	Approximately 50 MB – 100 MB memory and 1-5% CPU utilization,depending on user activity and screens.
Visibility Mode	Stealth or Visible
Deployment	• Silent MSI Installer • Deployment via Group Policy
Bandwidth	Approximately 30 kbps upstream depending on users activity and screens.
Offline Storage	Empmonitor also records activities offline and saves all data locally. This helps in case of network breakdown to upload the data of activities done during network breakdown period to the server.